UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/685,885	10/11/2000	Anders Johnson	108339-00010	5015

7590 11/01/2005

SQUIRE SANDERS & DEMPSEY LLP
14th FL
8000 Towers Crescent Drive
Tysons Corner, VA 22182-2700

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 11/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	Application No. 09/685,885	Applicant(s) JOHNSON, ANDERS	
	Examiner Ponnoreay Pich	Art Unit 2135	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 11 October 2005 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-33*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See attached.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____
13. ☐ Other: _____.

DETAILED ACTION

Claims 1, 15, and 25 were amended and arguments were presented. Claims 4, 20, and 28 were cancelled. All these amendments were presented after final rejection was made.

Response to Arguments

Applicant's arguments filed 10/11/2005 have been fully considered but they are not persuasive.

Applicant argues for claim 1 that Tello and Angelo does not disclose *wherein said at least one memory further comprises a guess register in communication with the host and the encryption module, the guess register being configured to receive a guess passcode from said host.* The examiner respectfully disagrees. This limitation was found in claim 4 before applicant cancelled claim 4 after final rejection was made. The examiner had cited col 24, lines 46-50 of Tello as meeting this limitation. The cited passage clearly shows a guess register being read and decrypted by the security engine microprocessor. The security engine microprocessor executes encryption/decryption algorithms, therefore it is an encryption module as well as being a decryption module. Further, in the context of Tello and Angelo's combination invention, it was stated that the host is configured to receive a guess passcode from a manufacturer of the component. The guess passcode is stored in the guess register, so only by being in communication with the host, either directly or indirectly, can the passcode get in the guess register to be read later by the security engine. The examiner notes that col 25, line 62-col 26, line 3 of Tello also reads on a guess register

in communication with the host, the guess register being configured to receive a guess passcode from said host. Note when the smart card is set up, the user enters personal information into the card. This entry is most likely done via the computer, i.e. host, seen in Fig 1.

Applicant argues for claim 15 that Tello and Angelo does not disclose *the encryption module comprises a public key encryption module, and a public key module in communication with the public key encryption module, wherein the public key encryption module is configured to receive a public key from the public key module and a guess passcode from the means for acquiring, and generate a ciphertext bit string therefrom*. The examiner respectfully disagrees. This limitation was found in claim 20 before application cancelled it after final rejection was made. The examiner cited passages from Tello to meet these limitations. Note col 15, lines 6-9 of Tello clearly discloses a public key encryption module. Col 15, lines 6-19 discloses the public key module in communication with said public key encryption module. If they were not in communication, public key encryption would not be possible since the public key encryption module would not have a public key to perform encryption with. Note further that col 5, lines 6-19 of Tello discloses that the use of public key cryptography is used to ensure that data flowing between the smart card reader and the security engine is secure. To enable devices, the identification data found in the smart card, i.e. guess passcode, must match what is stored by the security engine 123 (Fig 1). As this information must be sent from the smart card to the security engine for comparison, it

must be encrypted, generating a ciphertext bit string from the guess passcode, i.e. via public key encryption.

Applicant argues that Tello does not disclose *a hash function module in communication with a random number generating module* as recited in claims 1 and 15. Applicant argues that according to the present invention, the generated random number is transmitted to the input of hash function module as pre-image information and the hash function module receives a random number as an input and generates a hash value at the output of the hash function module. Applicant is reminded that although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The limitation being argued only recites a hash function module in communication with a random number generating module. An encryption module clearly reads on a random number generation module and the hash numbers are encrypted, therefore reads on the recited limitation.

Applicant argues for claim 25 that Davis, Tello, and Angelo do not disclose *a public key is received from a public key module, while a guess passcode is received from a guess register.* Applicant is reminded that although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The limitations applicant proposes to amend to claim 25 which is under consideration recite nothing about the public key being received from a public key module and a guess passcode is received from a guess register, only that a guess passcode is received

from a host and that a public key is received. Further, these proposed amendments would not overcome the prior art of record. Tello discloses receiving a public key (col 15, lines 6-20). Tello also discloses receiving a guess passcode from a host (col 25, line 62-col 26, line 3).

Applicant argues Davis, Tello, and Angelo do not disclose the amended limitation: *encrypting the guess passcode and the public key to generate a ciphertext bit string.* Applicant is directed to col 13, lines 55-63 of Davis where a serial number is encrypted with a control password key to produce a derived password. The derived password is then encrypted once more to establish a password cryptogram. Note the derived password is the combination of a guess passcode and an encryption key. Further, public keys were well known at the time applicant's invention was made and was disclosed by Tello (col 8, lines 33-40). Public keys are longer keys as compared to private keys and generally more secure. It would have been obvious to one of ordinary skill in the art to have the control password key be a public key because it would make the derived password longer when generated and more secure. Thus, applicant's proposed amendment to claim 25 would not overcome the prior art of record.

Applicant argues that Davis does not disclose that a second bit string corresponding to the random number is determined, i.e. as per the limitation of *determining a second bit string corresponding to the random number.* The examiner respectfully disagrees. "Determine" means to establish or ascertain definitely, as after consideration, investigation, or calculation. Col 13, lines 36-46 of Davis clearly discloses a security module which encrypts a random number. The output of the

encryption reads on a second bit string corresponding to the random number. This output was determined via calculation involving the random number, i.e. encryption calculation.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100